REMARKS/ARGUMENTS

Favorable consideration of this application, in light of the following discussion, is respectfully requested.

Claims 8-11 and 13-14 are pending.

In the Official Action Claims 8, 9, 13 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shamir (EP 0325238) in view of Schneier (Applied Cryptography Protocols, Algorithms and Source Code in C, 2nd Edition, pages 249 and 250); and Claims 10 and 11 were indicated as containing allowable subject matter.

Applicants acknowledge with appreciation the indication of allowable subject matter.

Briefly recapitulating, Claim 8 is directed to an authentication process involving a first device, which possesses a public key v and a secret key s, and a second device, which knows the public key v, the first and second entities being provided with means to exchange zero-knowledge information and to carry out cryptographic calculations on the zero-knowledge information. The public and secret keys are related by an operation modulo n, where n is an integer. The modulus n is specific to the first device. Calculations are carried out modulo n wherein in the process the modulo n operation is of $v=s^{-t} \pmod n$, t is a parameter and the modulo n calculations are performed according to the "Chinese remainders" method. The modulus n is the product of two primes of similar size.

Shamir describes a residue modulo n calculation. However, as noted in the Official Action, Shamir is silent about the use of the Chinese remainder. Schneier discloses a variety of cryptography protocols and discloses the use of the Chinese Remainder theorem. However, Schneier fails to disclose or suggest using the Chinese Remainder theorem in an authentication process. Applicants submit that a person having an ordinary skill in the art would not find in Schneier any indication or suggestion to perform the residue modulo n

calculation in Shamir's invention by means of calculation according to the Chinese remainder method.

In the claimed invention, the Chinese remainder theorem is used ***only*** with primes of similar magnitude. Shamir does not disclose ***any*** use of the Chinese remainder theorem, let alone use of a Chinese remainder theorem with primes of similar magnitude. Scheiner is applied for a teaching of the use of the Chinese remainder theorem. However, it is not clear how the primes from Shamir would be used with the Chinese remainder theorem of Scheiner. Thus, Applicants submit that the outstanding rejection does little more than attempt to show that parts of the inventive combination of Claim 8 were individually known in other arts and to suggest that such a showing is all that is necessary to establish a valid case of *prima face* obviousness. The PTO reviewing court recently reviewed such a rationale and dismissed it in *In re Rouffet*, 149 F. 3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998) as follows:

> "As this court has stated, "virtually all [inventions] are combinations of old elements." *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 698, 218 USPQ 865, 870 (Fed. Cir. 1983); see also *Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1579-80, 219 USPQ 8, 12 (Fed. Cir. 1983) ("Most, if not all, inventions are combinations and mostly of old elements."). Therefore an examiner may often find every element of a claimed invention in the prior art. If identification of each claimed element in the prior art were sufficient to negate patentability, very few patents would ever issue. Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to determine patentability." *Sensonics, Inc. v. Aerosonic Corp.*, 81 F.3d 1566, 1570, 38 USPQ2d 1551, 1554 (Fed. Cir. 1996). To prevent the use of hindsight based on the invention to defeat patentability of the invention, this court requires the examiner to show a motivation to combine the references that create the case of obviousness. In other words, the examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. [emphasis added.]

Applicants submit no such showing has been made.

Applicants also note that the rejection is based upon an example disclosed in Shamir in which n is taken equal to the product of two prime numbers p and g, where p=3 mod 8 and g=7 mod 8, so that public keys vj are automatically quadratic residues mod n. Applicants submit this mathematical characteristic is different from the one claimed in the present invention in which prime numbers p and g are of **similar size**. Using Shamir's criterion, one can consider for example p=3 and g=8*100,000+7=80007, such that g is 200,000 times greater than p. Consequently, in the example of Shamir p and g do not necessarily result in a **similar size** as is required by Applicants' claimed invention. However, Applicants also concede that, while Shamir does not disclose primes of similar magnitude, Shamir also does not preclude primes of similar magnitude.

MPEP § 2144.05 (Obviousness of Ranges) recites "In the case where the claimed ranges "overlap or lie inside ranges disclosed by the prior art" a *prima facie* case of obviousness exists. MPEP § 2144.05 further recites "Applicants can rebut a *prima facie* case of obviousness based on overlapping ranges by showing the criticality of the claimed range. "The law is replete with cases in which the difference between the claimed invention and the prior art is some range or other variable within the claims. . . . In such a situation, the applicant must show that the particular range is critical, generally by showing that the claimed range achieves unexpected results relative to the prior art range." *In re Woodruff*, 919 F.2d 1575, 16 USPQ2d 1934 (Fed. Cir. 1990)."

MPEP § 716.02 (Allegations of Unexpected Results) recites "Any differences between the claimed invention and the prior art may be expected to result in some differences in properties. The issue is whether the properties differ to such an extent that the difference is really unexpected. *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986) (differences in sedative and anticholinergic effects between prior art and claimed

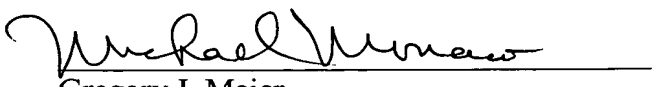
antidepressants were not unexpected). In *In re Waymouth*, 499 F.2d 1273, 1276, 182 USPQ 290, 293 (CCPA 1974), the court held that unexpected results for a claimed range as compared with the range disclosed in the prior art had been shown by a demonstration of "a marked improvement, over the results achieved under other ratios, as to be classified as a difference in kind, rather than one of degree." Compare *In re Wagner*, 371 F.2d 877, 884, 152 USPQ 552, 560 (CCPA 1967) (differences in properties cannot be disregarded on the ground they are differences in degree rather than in kind); *Ex parte Gelles*, 22 USPQ2d 1318, 1319 (Bd. Pat. App. & Inter. 1992) ("we generally consider a discussion of results in terms of 'differences in degree' as compared to 'differences in kind' . . . to have very little meaning in a relevant legal sense")."

In the present case, Shamir's use of primes includes the use of primes of similar magnitude. Thus, the range claimed in the pending claims is encompassed within the range disclosed by Shamir. However, the use of the Chinese remainder leads to an acceleration of calculation by factor ranging from 3 to 4 or 1, 5 to 2 depending on the size of e with regard to n and to p. Furthermore, when the number of primes factors (of similar sizes) is larger than 2 and equal to k, the acceleration factor is nearing k^2 in the first case (e and n of similar size) and close to k in the seconds case (e is lower than or equal to p). When p and q are of similar size, each of the calculations (y_p and y_q) is about ***8 times faster*** than the calculation of $y = x^e \pmod n$ when n and e are of similar size, ***4 times faster*** when the size of e is lower or equal to the size of p. This increase in speed was unexpected by the inventors and meets the criteria of MPEP § 716.02. The restriction of the size of the primes to sizes of similar magnitude is critical to the claimed invention, meeting the criteria of MPEP § 2144.05. If desired, Applicants will file a declaration per MPEP § 716.02(g) signed by one or more of the inventors to substantiate the above assertions.

Accordingly, in light of the previous discussion, Applicants respectfully submit that the present application is in condition for allowance and respectfully request an early and favorable action to that effect.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599

Michael E. Monaco
Registration No. 52,041

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\MM\AMENDMENT\2623\211526US.RESP DUE 7-18-06.DOC